

Datensicherheit fürs Firmennetz

## Endpoint Data Protection 2011 von Cynapspro im Usability-Test

04.05.2011 | Autor: Götz Güttich



Endpoint Data Protection 2011 von Cynapspro beherrscht die wichtigsten Disziplinen der Datensicherheit.

**Mobile Speichermedien stellen für Netzwerk und Administrator ein nicht zu unterschätzendes Risiko dar. Sie eignen sich für Datendiebstahl, beherbergen mitunter Malware und gehen häufig verloren, so dass Informationen leicht in die Hände Unbefugter geraten. Cynapspro entwickelt Security-Tools für genau diesen Problembereich. Doch was leisten die Werkzeuge in der Praxis?**

Die Sicherheitssuite Endpoint Data Protection 2011 von Cynapspro besteht aus mehreren unterschiedlichen Komponenten, die sich alle über eine zentrale Managementkonsole verwalten lassen. Das Tool DevicePro ist der wohl wichtigste Bestandteil der Cynapspro-Produktreihe. Dieses Werkzeug steuert den Datentransfer von und zu externen Speichermedien wie USB-Sticks und externen Festplatten.

Dafür behält es unter anderem Datenübertragungen über Systemports, WLAN-Netze und optische Speichermedien im Auge und kann bestimmte Medien (wie etwa ausgewählte CDs) zulassen und andere abblocken. Darüber hinaus haben Administratoren mit DevicePro die Möglichkeit, Übertragungen bestimmter Datentypen auf externe Medien zu unterbinden oder zu erlauben.

Sämtliche Rechte lassen sich den verwalteten Computern und Benutzern in Echtzeit zuweisen, darüber hinaus bietet die Lösung auch Unterstützung für mobile User. Umfassende Protokoll-Funktionen sorgen schließlich dafür, dass alle Arbeitsschritte nachvollziehbar sind, so dass die Anwender der Software keine Probleme beim Einhalten behördlicher Vorgaben bekommen.

### BILDERGALERIE



Fotostrecke starten: Klicken Sie auf ein Bild (7 Bilder)

Als zweite wichtige Komponente verschlüsselt CryptionPro die Daten auf mobilen Speichergeräten automatisch, so dass sich Anwender um diesen Teil der Datensicherung nicht selbst kümmern müssen. Die Verschlüsselung erfolgt auf Dateiebene. Bei Bedarf ist es also ohne großen Aufwand möglich, einzelne Dateien unverschlüsselt herauszugeben. Eine „mobile Verschlüsselung“ schützt gleichzeitig alle Daten, die ein externer Mitarbeiter außerhalb des Unternehmens erhält.

Die Passwortverwaltung läuft über eine zentrale Stelle ab, die Zugriffsrechte lassen sich nach Benutzern und Gruppen zuteilen. Bei den weiteren Komponenten der Suite – auf die wir hier nur am Rande eingehen – handelt es sich um eine Festplattenverschlüsselung, ein Tool zum Blockieren unerwünschter Anwendungen, ein Werkzeug zum sicheren Löschen von Daten und eine Komponente zum Einsparen von Energiekosten.

## Installation

Alle Komponenten der Security-Suite von Cynaspro werden wie erwähnt über eine zentrale Konsole verwaltet und greifen auf eine gemeinsame Datenbank zu, die sämtliche Informationen vorhält. Der Hersteller empfiehlt als Datenbank den SQL Server Express von Microsoft.

Wir hielten uns an diese Empfehlung und spielten die Version 2005 der genannten Datenbank auf einem Rechner ein, der unter Windows Server 2003 R2 mit Service Pack 2 in der 32-Bit-Version lief. Dieser Computer kam dann später auch zum Einsatz, um die Sicherheitstools und die zentrale Managementkonsole zum Laufen zu bringen.

In diesem Zusammenhang ist positiv zu vermerken, dass neben der SQL-Datenbank keine weiteren Komponenten zum Betrieb der Endpoint Data Protection 2011 erforderlich sind. Folglich entstehen auch keine neuen Sicherheitslücken und keine versteckten Kosten.

Sobald die Datenbank läuft, kann man den Setup-Assistenten von DevicePro aufrufen. Dieser möchte neben der Sprache und dem Installationspfad im Wesentlichen wissen, ob er Benutzerdaten aus einem Active- oder einem E-Directory sowie aus einem Open-LDAP-Verzeichnis importieren soll.

Während des Setups erfolgt das Vorbereiten der Verzeichnissynchronisation. Hierfür genügt es, der Software die Anmeldedaten eines Benutzerkontos mitzuteilen, das die relevanten Daten aus dem jeweiligen Verzeichnisdienst auslesen darf. Die weitere Konfiguration der Verzeichnisdienst-Integration wird dann im Betrieb über die Management-Konsole vorgenommen. Wurden alle Angaben gemacht, so läuft die Installation durch und auf dem Desktop des Rechners erscheint ein Icon zum Zugriff auf die Managementkonsole.

## Inhalt

Seite 1: Installation

Seite 2: **Erste Konfiguration**

Seite 3: **Der Funktionsumfang**

Seite 4: **Encryption-Optionen**

Seite 5: **Konfiguration der Verschlüsselung**

Seite 6: **Konfiguration der Suite**

**Datensicherheit fürs Firmennetz**

# Endpoint Data Protection 2011 von Cynaspro im Usability-Test

04.05.2011 | Autor: Götz Güttich

## Erste Konfiguration

Nach dem Setup kann der Benutzer, der die Installation durchgeführt hat, das Verwaltungswerkzeug als Supervisor starten. Danach erscheint ein Willkommensbildschirm mit vier Konfigurationsschritten, die erforderlich sind, um die Software in Betrieb zu nehmen.

Administratoren erhalten also – ähnlich wie bei neueren Windows- Servern – nach dem Setup eine To-Do-Liste. Diese müssen sie für eine erfolgreiche Grundkonfiguration lediglich abarbeiten. Wir halten diesen Ansatz für sehr gelungen, da dabei praktisch nichts schiefgehen kann.

Der erste Konfigurationsschritt dient dazu, die Standardbenutzerrechte festzulegen, die ein neues Benutzerkonto erhält, sobald es in der Cynaspro-Umgebung erscheint. Defaultmäßig erhalten an dieser Stelle alle User alle Rechte, deswegen wird es in den meisten Umgebungen sinnvoll sein, die Standardrechte so einzuschränken, dass wirklich nur Zugriff auf die unbedingt benötigten Komponenten besteht.

Im nächsten Schritt führen die IT-Mitarbeiter eine Synchronisation mit dem im LAN vorhandenen Verzeichnisdienst durch (bei uns war das das Active Directory auf einem Server unter Windows Server 2008 R2). Auf diese Weise machen sie der Lösung von Cynaspro die vorhandenen Benutzerkonten bekannt und diese erhalten gleich auch die eben definierten Standardbenutzerrechte.

### **Vergebene Rechte nachträglich anpassen**

Nachdem die Benutzerkonten im System vorhanden sind, geht es daran, die Rechte einzelner User an die Sicherheitsanforderungen im Unternehmen anzupassen. Beispielsweise ist es oft sinnvoll, bestimmten Anwendern Zugriff auf optische Speichermedien oder ähnliches zu geben.

Sobald alle Benutzerrechte den Vorstellungen der Administratoren entsprechen, generieren die zuständigen Mitarbeiter im letzten Schritt eine MSI-Datei, mit der sich der Agent der Sicherheitssuite auf den verwalteten Rechnern installieren lässt. Hierbei gibt es unter anderem die Option, das Tray-Icon des Agenten auf den Clients zu verstecken, so dass die User die Software überhaupt nicht zu Gesicht bekommen.

Abgesehen davon sind die IT-Verantwortlichen dazu in der Lage, das Stoppen des Sicherheitsdienstes durch den lokalen Administrator auf den Clients zu unterbinden (was in den meisten Fällen sinnvoll sein dürfte) und ein Passwort zu definieren, das ein Administrator vor dem Entfernen des Agenten von einem verwalteten System eingeben muss.

Last but not Least besteht auch die Option, Benutzerrechte und Freigaben mit in die Installationsdatei zu integrieren. Nach dem Abschluss der dazugehörigen Konfiguration erstellt die Verwaltungskonsole dann MSI-Files für 32- und 64-Bit-Windows-Systeme, die sich anschließend im Netzwerk verteilen lassen.

Im Test spielten wir den Agenten zunächst auf einem 64-Bit-System unter Windows 7 und dann auf einem 32-Bit Windows-XP-Rechner mit Service Pack 3 ein. Dabei kam es zu keinen Überraschungen und wir verfügten anschließend über eine einsatzbereite Umgebung.

### **Inhalt**

Seite 1: **Installation**

Seite 2: Erste Konfiguration

Seite 3: **Der Funktionsumfang**

Seite 4: **Encryption-Optionen**

Seite 5: **Konfiguration der Verschlüsselung**

Seite 6: **Konfiguration der Suite**

**Datensicherheit fürs Firmennetz**

## **Endpoint Data Protection 2011 von Cynaspro im Usability-Test**

04.05.2011 | Autor: Götz Güttich

### **Der Funktionsumfang**

Wenden wir uns nun dem Funktionsumfang der Sicherheitssuite zu. Die Cynaspro-Verwaltungskonsole verfügt über eine Menüzeile, über die sich die Administratoren mit bestimmten DevicePro- Servern verbinden können. An

gleicher Stelle ist es auch möglich, die Ansicht anzupassen, eine Suchfunktion aufzurufen und die Sprache umzustellen. An Sprachen unterstützt das System Englisch und Deutsch. Unter der Menüzeile befindet sich eine Icon-Leiste, über die die Anwender die wichtigsten Befehle aufrufen.

Interessanter ist die Menüstruktur auf der linken Fensterseite, über die sich sämtliche Features des Tools ansprechen lassen. Die eigentliche Konfiguration findet dann im Arbeitsfenster rechts davon statt. Der wohl wichtigste Punkt des Menüs dürfte das „Device Management“ sein, denn hier legen die zuständigen Mitarbeiter fest, wer auf welches Gerät zugreifen darf und wer nicht.

Dabei haben sie nicht nur Gelegenheit, die eben bereits erwähnten Standardrechte für neue Benutzer zu definieren, sondern sind auch dazu in der Lage, Zugriffsrechte für ausgewählte Benutzerkonten oder Computer zu definieren. Es existieren bei DevicePro also nicht nur rechnerbasierte Rechte wie „Auf PC1 darf niemand das DVD-Laufwerk nutzen“, sondern auch Rechte, die mit Benutzerkonten verknüpft sind („User1 darf auf allen oder bestimmten Systemen externe Speichermedien nutzen“).

## **Geräte- und Schnittstellen-Konfiguration**

Gehen wir jetzt etwas genauer auf die Definition der Zugriffsrechte für Geräte ein. Am Devices unterstützt DevicePro unter anderem Floppy-Disks, optische Speichermedien, USB-Komponenten, SD/MMC-Karten, IrDA- und Bluetooth-Geräte, Wifi- und Firewire-Schnittstellen, parallele und serielle Ports, PCMCIA-Karten, PDAs, ISDN-Karten, Modems, Drucker, Scanner, Kameras sowie Game-Controller.

In der Zugriffsverwaltung finden die zuständigen Mitarbeiter eine Liste mit Device-Typen, wie eben CD/DVD-Laufwerke, externe Speicher, Blackberrys und so weiter. Die gewünschten Zugriffsrechte passen sie dann durch einen Rechtsklick auf den jeweiligen Listeneintrag an (Vollzugriff, nur Lesen, kein Zugriff). Zusätzlich sind sie auch dazu in der Lage, den Gerätezugriff nur zu bestimmten Zeiten freizugeben und einmalige Freigaben durchzuführen.

Für die auf dem jeweiligen Client-System vorhandenen Ports – also Firewire- und PCMCIA-Schnittstellen oder andere – lassen sich ähnliche Einstellungen vornehmen, wie für die Devices. Im Betrieb haben die Portsettings eine höhere Priorität als die Geräteeinstellungen.

Zusätzlich zu den genannten Punkten existiert unter anderem auch noch ein Notfall-Dialog, über den die IT-Verantwortlichen alle Zugriffe sofort sperren können. Im Test gelangten wir zu dem Ergebnis, dass die Rechtezuweisung klar und übersichtlich gegliedert wurde und kaum jemanden vor irgendwelche Probleme stellen dürfte.

Über den Reiter „Revision“ bietet DevicePro Informationen darüber an, welche Rechte wann vom wem aus welchem Grund geändert wurden, während die Protokollierung alle Datenbewegungen aufzeichnet. Sie bietet also unter anderem Informationen zu gelesenen, umbenannten und geschriebenen Dateien und ist zudem dazu in der Lage, Schattenkopien aller Daten – sogar von Druckaufträgen - für spätere Analysen bereitzustellen.

Die Protokollierungsfunktion ist demzufolge sehr mächtig und kann leicht die Privatsphäre der Nutzer verletzen. Deswegen lässt sie sich mit zwei Passwörtern absichern, um beispielsweise dafür zu sorgen, dass der Betriebsrat des Unternehmens beim Zugriff auf die Daten beteiligt werden muss.

## **Inhalt**

Seite 1: **Installation**

Seite 2: **Erste Konfiguration**

Seite 3: Der Funktionsumfang

Seite 4: **Encryption-Optionen**

Seite 5: **Konfiguration der Verschlüsselung**

## Endpoint Data Protection 2011 von Cynapspro im Usability-Test

04.05.2011 | Autor: Götz Güttich  
**Encryption-Optionen**

Im Konfigurationsbereich für CryptionPro legen die Administratoren die Verschlüsselungsoptionen für Benutzerkonten fest. Hierbei stehen zur Wahl „Allgemeine Verschlüsselung“, „Gruppenverschlüsselung“, „Individuelle Verschlüsselung“ und „Mobile Verschlüsselung“.

Die allgemeine Verschlüsselung sichert die Daten mit einem Unternehmens- Key, das bedeutet, jeder Unternehmensmitarbeiter kann sie wieder entschlüsseln.

Bei der Gruppenverschlüsselung kommt ein Gruppen-Key zum Einsatz. In diesem Zusammenhang ist es beispielsweise denkbar, alle Mitarbeiter einer Abteilung – etwa die Personalabteilung - zu einer Gruppe zusammenzufassen und für diese einen gemeinsamen Key zu erzeugen, mit dem sie ihre Dokumente gegenseitig einsehen können, ohne dass die anderen Mitarbeiter darauf Zugriff erhalten.

Die individuelle Verschlüsselung ermöglicht es nur dem Benutzer, der die Daten verschlüsselt hat, später wieder darauf zuzugreifen.

Derweil versetzt die mobile Verschlüsselung die Mitarbeiter in die Lage, Daten außerhalb des Unternehmensnetzes mit einer portablen Exe-Datei, die von der Cynapspro-Installation unabhängig ist, zu ver- bzw. entschlüsseln.

Im Betrieb haben die User dann Gelegenheit, ihre Daten mit den für sie vom Administrator freigegebenen Verschlüsselungsoptionen zu sichern. Es ist sogar möglich, Benutzern das Recht zuzugestehen, Daten überhaupt nicht zu verschlüsseln.

Die Verschlüsselung lässt sich also bei Bedarf jederzeit erzwingen oder deaktivieren. Im Test traten dabei keine Probleme zu Tage. Unserer Meinung nach handelt es sich bei der CryptionPro um ein sehr sinnvolles Tool, da es das Datensicherheitsniveau deutlich verbessert, ohne die Anwender mit zusätzlichen Arbeitsschritten zu belasten.

Ebenfalls von Interesse ist der Content Filter, denn mit dieser Funktion können die zuständigen Mitarbeiter die Übertragung bestimmter Dateien nach Typ, Name und Größe unterbinden. Der Dateityp wird dabei über seinen Hashwert festgestellt, so dass das Umbenennen bestimmter Files – beispielsweise von {Dateiname}.ppt zu {Dateiname}.txt – nicht ausreicht, um das System auszuhebeln. Der Hersteller hat in diesem Zusammenhang praktisch alle relevanten Dateitypen bereits vordefiniert. Im Bedarfsfall lassen sich aber **mit dem Tool Winhex eigene Definitionen erstellen**.

Der letzte Punkt des Device Managements befasst sich mit der Verwaltung von WLANs. Hier legen die IT-Verantwortlichen fest, wann die Anwender welche WLANs nutzen dürfen, und zwar nach Verschlüsselungsmethode, SSID, Name sowie IP- und MAC-Adressen.

## Inhalt

Seite 1: **Installation**

Seite 2: **Erste Konfiguration**

Seite 3: **Der Funktionsumfang**

Seite 4: **Encryption-Optionen**

Seite 5: **Konfiguration der Verschlüsselung**

Seite 6: **Konfiguration der Suite**

**Datensicherheit fürs Firmennetz**

# Endpoint Data Protection 2011 von Cynaspro im Usability-Test

04.05.2011 | Autor: Götz Güttich

## Konfiguration der Verschlüsselung

Im Konfigurationsmenü „Verschlüsselung“ nehmen die zuständigen Mitarbeiter sämtliche Einstellungen für CryptionPro vor, die dann im eben erwähnten Device Management zum Einsatz kommen können. Das heißt, hier lassen sich die Verschlüsselungsfunktionen für externe und interne Speichermedien aktivieren beziehungsweise definieren.

Bei den externen Speichermedien können Administratoren beispielsweise die erwähnten Verschlüsselungseinstellungen wie „Allgemeine Verschlüsselung“ und „Mobile Verschlüsselung“ für die Verschlüsselungskonfiguration innerhalb des Device Managements bereitstellen. Darüber hinaus wählen die zuständigen Mitarbeiter hier auch die gewünschte Verschlüsselungsmethode aus. CryptionPro bietet dazu AES256 und – für Windows-2000-Systeme – Triple DES an.

Ebenfalls von Interesse: die Schlüsselverwaltung, die den Export und Import von Schlüsseln ermöglicht, die Gültigkeitsdauer der Schlüssel festlegt, das automatische Anlegen neuer Schlüssel steuert und das Erzeugen eines Master-Schlüssels realisiert, mit dem sich über den Befehl „Daten-Wiederaufnahme“ alles entschlüsseln lässt. Auch hierbei ergaben sich im Test keine Probleme.

Die nächsten Punkte der Verschlüsselungskonfiguration sind schnell erklärt: Sie umfassen eine Gruppenverwaltung zum Anlegen von Verschlüsselungsgruppen, die mehrere Benutzerkonten mit einem einheitlichen Schlüssel zusammenfassen, eine Geräte-Blacklist und die Einstellungen zu CryptionPro Mobile.

Letztere enthalten unter anderem die Passwortsicherheitsrichtlinie, die festlegt, welche Zeichen das Passwort enthalten muss und wie lang es werden soll. Im Test waren die Verschlüsselungseinstellungen schnell vorgenommen und das System verhielt sich anschließend wie erwartet.

## Geräte- und Medienfreigabe

Mit Hilfe der Gerätefreigabe können die Administratoren bestimmte Geräte nach Typen (also CD/DVD, serieller Port, Diskettenlaufwerk, externer Speicher und so weiter) freigeben. An dieser Stelle existiert auch die Option, die Client-Rechner zu scannen und so zu sehen, welche Devices wo vorhanden sind.

Die gefundenen Geräte landen dann in der Datenbank und die zuständigen Mitarbeiter erhalten Gelegenheit, einzelne Geräte individuell freizugeben. Da das System die Gerätedaten in der eben genannten Datenbank vorhält, müssen die Client-Systeme zum Freigeben bestimmter Komponenten nicht online sein und es ist möglich, einzelne Devices in der Datenbank zu suchen.

Zusätzlich besteht auch die Option, die Arbeit mit bestimmten Medien zuzulassen: So sorgt die Medienfreigabe

beispielsweise dafür, dass Anwender auf bestimmte, zuvor definierte CDs zugreifen können, auf andere aber nicht. Im Test ergaben sich dabei keinerlei Schwierigkeiten.

An gleicher Stelle lassen sich auch Challenge-Response-Freigaben mit Anfrage- und Freigabe-Code und Rechten wie Voll- oder Nur-Lese-Zugriff realisieren. WLAN-Freigaben schließen die Konfiguration der Gerätefreigaben ab. Sie ermöglichen das Freigeben bestimmter Funknetze für einzelne Rechner oder das ganze Unternehmen. WLANs, die in der Freigabe nicht aufgeführt sind, werden ausnahmslos gesperrt.

Über die Liste der DevicePro-Agenten, die sich innerhalb der Menüstruktur findet, wählen die zuständigen Mitarbeiter übrigens immer aus, auf welchem System die Gerätefreigaben Gültigkeit haben. Auf diese Weise verhindert die Managementkonsole versehentliche Freigaben auf den falschen Systemen.

## Inhalt

Seite 1: **Installation**

Seite 2: **Erste Konfiguration**

Seite 3: **Der Funktionsumfang**

Seite 4: **Encryption-Optionen**

Seite 5: Konfiguration der Verschlüsselung

Seite 6: **Konfiguration der Suite**

**Datensicherheit fürs Firmennetz**

## Endpoint Data Protection 2011 von Cynaspro im Usability-Test

04.05.2011 | Autor: Götz Güttich

### Konfiguration der Suite

Das Administrationsmenü umfasst alle Punkte zum Verwalten der Cynaspro Endpoint Data Protection selbst. Hier legen die Administratoren fest, wer das Recht erhält, die Konfiguration der Suite zu ändern oder auszulesen. Es ist auch möglich, einzelnen Benutzern nur den Zugriff auf Teile des Konfigurationswerkzeugs zu gewähren, wie etwa das Device Management oder die Medienfreigabe.

Außerdem lassen sich im Bereich Administration Mail-Alerts konfigurieren, Regeln zum Löschen alter Einträge aus der Datenbank einrichten und die Protokollierung aktivieren. An gleicher Stelle finden sich auch

die bereits angesprochene Definition der Contentheader-Filter zum Ausfiltern bestimmter Dateitypen und die Serververwaltung, mit der die IT-Mitarbeiter in Umgebungen mit mehreren DevicePro-Servern festlegen, welcher Server die Priorität beim Verwalten der Agenten erhält.

Bei der Clientverwaltung legen die Verantwortlichen die bei der Installation bereits beschriebenen Parameter für die Agenten-Installationsdateien fest und erzeugen anschließend – ebenfalls im Administrationsmenü – die erforderlichen MSI-Pakete.

Abgesehen davon ist es im genannten Menü auch noch möglich, Agenten von der Konsole aus zu installieren oder zu aktualisieren. Dabei lassen sich – für größere Umgebungen – die Zahl der gleichzeitigen Downloads und die Netzwerkauslastung begrenzen, so dass Update-Vorgänge das Unternehmensnetz nicht lahm legen können. Im Test hinterließ das Administrationsmenü einen aufgeräumten Eindruck.

## Das Reporting

Der letzte Punkt der Konsole enthält diverse Auswertungen, die den zuständigen Mitarbeitern einen Überblick über die Vorkommnisse in ihrem Netz geben. Dazu gehören eine Managementübersicht, die zeigt auf welchen Rechnern die Sicherheitssoftware läuft und auf welchen nicht, eine Liste nicht aktualisierter Rechte (mit Benutzer, Kontext, Datum und Änderung) sowie eine Auflistung aktiver und inaktiver Benutzer.

Darüber hinaus liefert die Software eine Analyse der Rechteveränderungen, eine Rechteübersicht, die die Rechte aller Benutzer auf Geräteklassen umfasst und eine zusammenfassende Rechteübersicht für Device-Klassen, die Aufschluss darüber gibt, wie viele Anwender auf ein Gerät Zugriff haben und wie viele nicht. Dank der umfassenden Auswertungsmöglichkeiten haben alle zuständigen Mitarbeiter jederzeit Gelegenheit, sich genau über den Zustand ihres Netzwerks zu informieren.

## **Zusammenfassung und Fazit**

Im Test installierten wir Cynaspro Endpoint Data Protection in unserem Netz und sicherten diverse Client-Rechner gegen unerwünschte Datenübertragungen ab. Die Software versah im alltäglichen Betrieb klaglos ihren Dienst.

Die meisten Einstellungen sind selbsterklärend, die Regeldefinition für Computer- und Benutzerregeln geht flott von der Hand und wir erzielten immer in kürzester Zeit die Ergebnisse, die wir uns bei der Konfiguration gewünscht hatten. Besonders positiv fiel uns auf, dass Konfigurationsänderungen sofort auf den Clients aktiv werden. Weitere Funktionen, wie Challenge-Response-Freigaben funktionierten stets ohne Schwierigkeiten.

Was CryptionPro angeht, so verschlüsselten wir im Test diverse externe Speichermedien, transportierten die Daten und entschlüsselten sie auf dem Zielsystem wieder. Dabei kam es ebenfalls zu keinen Überraschungen. Wir testeten zudem auch die unterschiedlichen Verschlüsselungsmethoden mit den allgemeinen Schlüsseln, sowie den individuellen und den Gruppen- Keys. Dabei traten keine Probleme auf. Folglich gilt CryptionPro als sinnvolles Werkzeug zum Absichern von Daten auf mobilen Speichermedien.

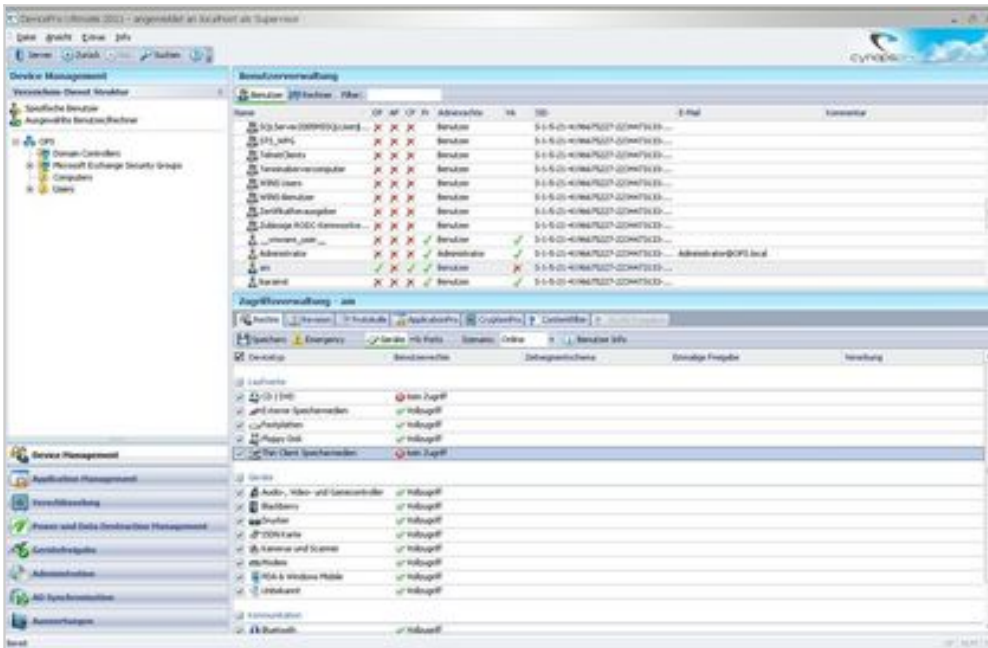
Ebenfalls positiv hervorzuheben sind die umfassenden Protokollierungs- und Auswertungsfunktionen. Diese sorgen nicht nur dafür, dass Unternehmen ohne großen Zusatzaufwand in die Lage versetzt werden, behördliche Vorgaben zu erfüllen, sondern stellen auch sicher, dass Administratoren jederzeit genau wissen, was in ihren Netzwerken vorgeht. Unter Berücksichtigung aller relevanten Aspekte kommen wir zu dem Schluss, dass es sich bei der Endpoint Data Protection von Cynaspro um ein durchaus empfehlenswertes Produkt handelt.

## **Inhalt**

Seite 1: [Installation](#)  
Seite 2: [Erste Konfiguration](#)  
Seite 3: [Der Funktionsumfang](#)  
Seite 4: [Encryption-Optionen](#)  
Seite 5: [Konfiguration der Verschlüsselung](#)  
Seite 6: Konfiguration der Suite  
Redakteur: Stephan Augsten

Dieser Beitrag ist urheberrechtlich geschützt.  
Sie wollen ihn für Ihre Zwecke verwenden?  
Infos finden Sie unter [www.mycontentfactory.de](http://www.mycontentfactory.de).

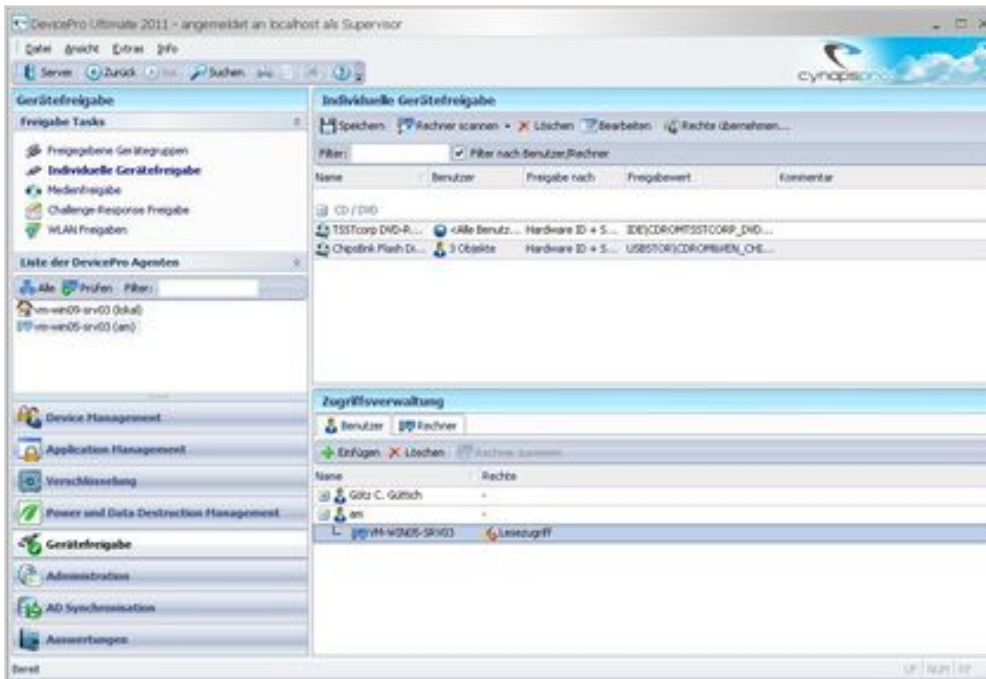




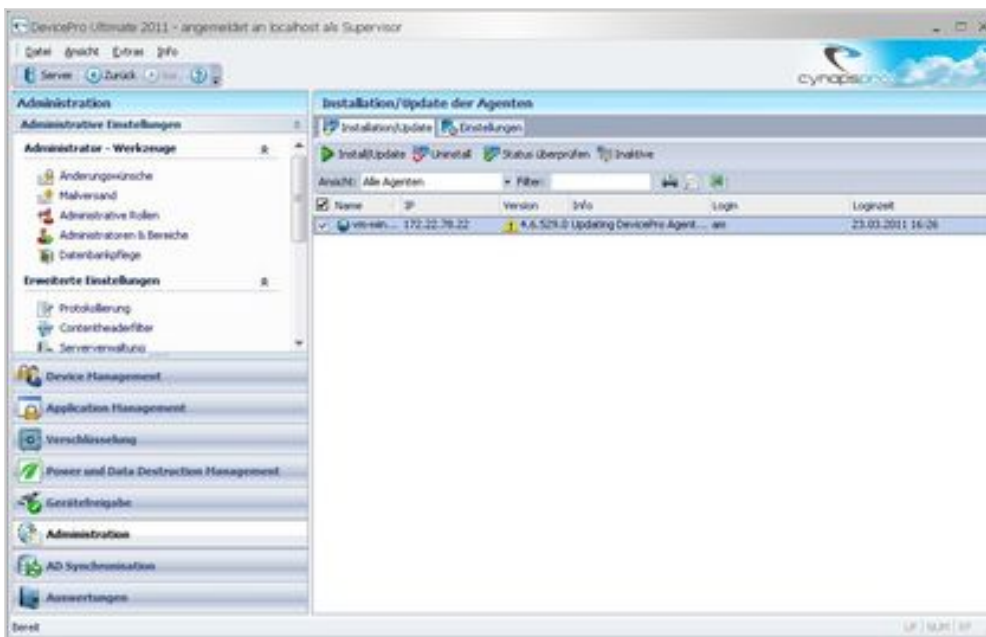
Über das Device Management weisen die zuständigen Mitarbeiter Zugriffsrechte auf Computer- und Benutzerebene zu.



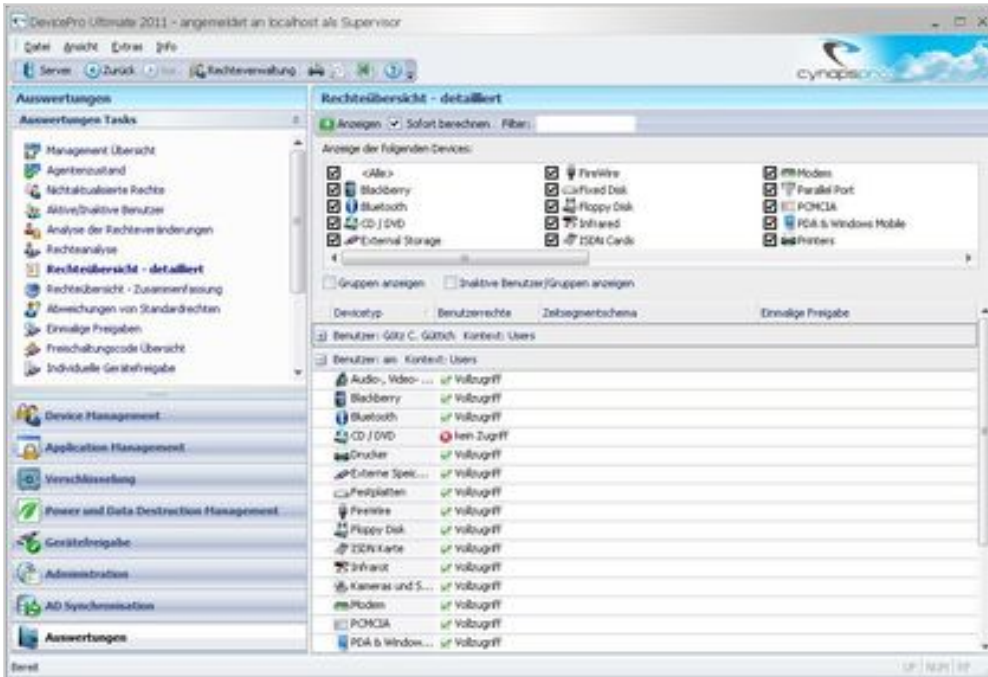
Mithilfe der Verschlüsselungseinstellungen lassen sich bestimmte Verschlüsselungstypen für die Anwender freigeben.



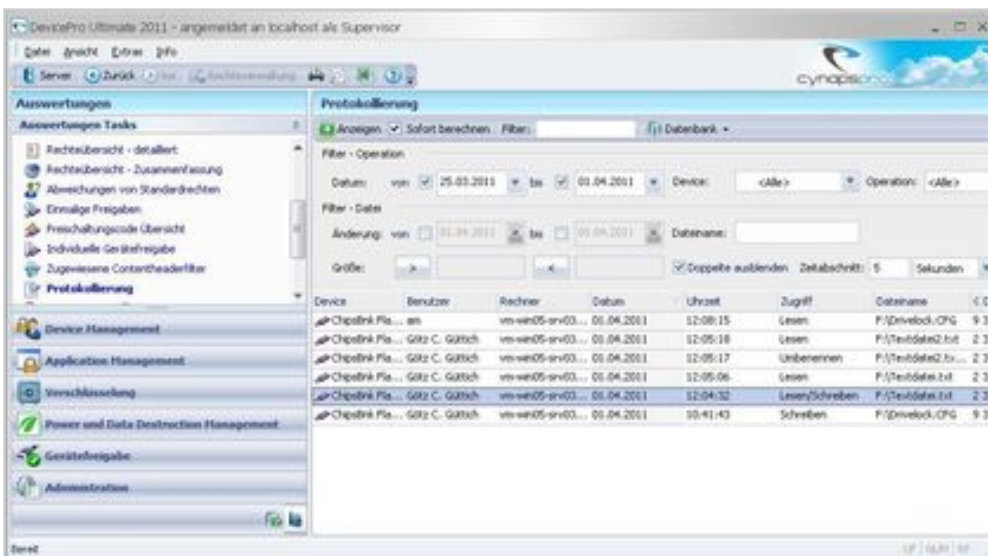
Die individuelle Gerätefreigabe ermöglicht das schnelle Freigeben bestimmter Komponenten.



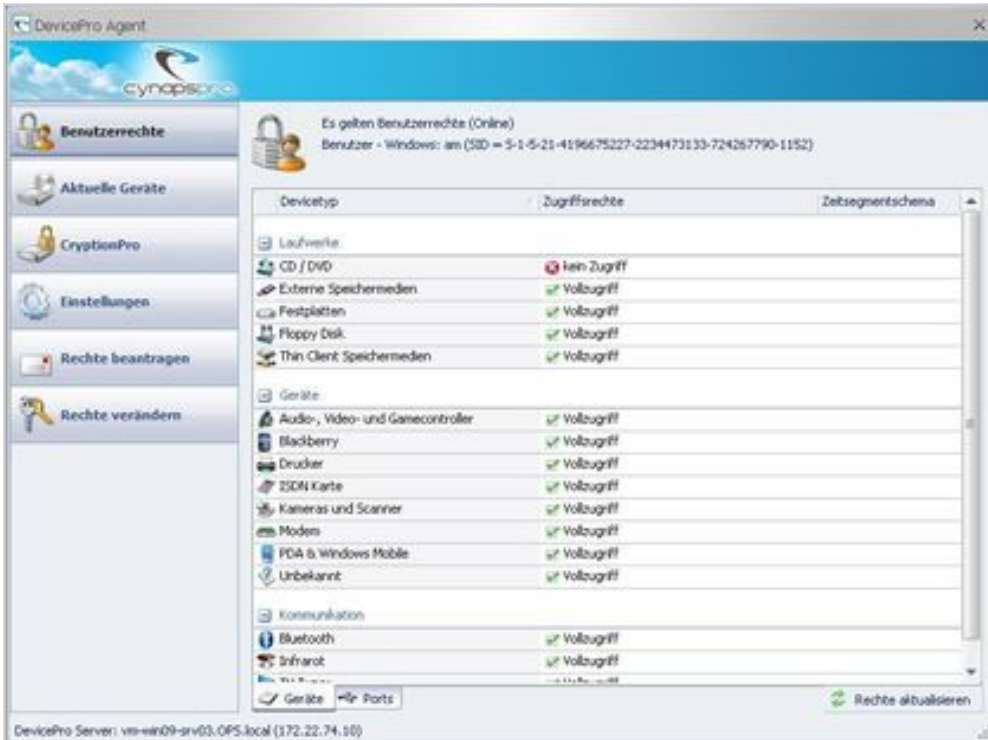
Bei Bedarf lassen sich die auf den Clients vorhandenen Agenten über die Verwaltungskonsole aktualisieren.



Dank der detaillierten Rechteübersicht erhalten Administratoren einen schnellen Überblick über den Rechtestatus in ihrem Netz.



Die Protokollierungsfunktion zeichnet alle Datenbewegungen auf.



The screenshot shows the 'DevicePro Agent' window with the 'Benutzerrechte' (User Rights) section active. It displays a table of permissions for the user 'Benutzer - Windows: am (SID = S-1-5-21-4196675227-2234473133-724267790-1152)'. The table lists device types and their corresponding access rights.

Devicetyp	Zugriffsrechte	Zeitsegmentschema
Laufwerke	kein Zugriff	
CD / DVD	kein Zugriff	
Externe Speichermedien	Vollzugriff	
Festplatten	Vollzugriff	
Floppy Disk	Vollzugriff	
Thin Client Speichermedien	Vollzugriff	
Geräte		
Audio-, Video- und Gamecontroller	Vollzugriff	
Blackberry	Vollzugriff	
Drucker	Vollzugriff	
ISDN Karte	Vollzugriff	
Kameras und Scanner	Vollzugriff	
Modem	Vollzugriff	
PDA & Windows Mobile	Vollzugriff	
Unbekannt	Vollzugriff	
Kommunikation		
Bluetooth	Vollzugriff	
Infrarot	Vollzugriff	

Buttons at the bottom: Geräte, Ports, Rechte aktualisieren.

Der DevicePro Agent gibt genauen Aufschluss darüber, welche Rechte der aktuell angemeldete Nutzer besitzt